UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

JOANNE ROMA, individually, and on behalf of all others similarly situated,	)	
Plaintiff	)	
V.	)	**Civil Action No. 2:23-cv-3216**
PROSPECT MEDICAL HOLDINGS, INC.	)	
Defendant	)	

COMPLAINT—CLASS ACTION

Plaintiff, JOANNE ROMA ("Plaintiff" or "Roma"), individually and on behalf of all others similarly situated, complains and alleges as follows against Defendant, Prospect Medical Holdings, Inc. ("Defendant" or "Prospect") based on personal knowledge, on the investigation of her counsel, and on information and belief as to all other matters:

INTRODUCTION

1. This is a civil action seeking monetary damages and injunctive and declaratory relief from Defendant Prospect Medical Holdings, Inc., arising from its failure to safeguard certain Personally Identifying Information[1] ("PII") and other sensitive, non-public financial information (collectively, "Personal Information") of thousands of its prospective, current, and former employees, resulting in a cyberattack of Defendant's network systems being unauthorizedly accessed on or about August 3, 2023. The Personal Information of employees therein, including

[1] The Federal Trade Commission defines "personally identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8). To be clear, according to Defendant, not every type of information included in that definition was compromised in the breach.

of Plaintiff and the proposed Class Members, has been and/or is currently being disclosed, stolen, compromised, and misused, causing widespread and continuing injury and damages.

2. On information and belief, on August 3, 2023, Prospect's network systems were unauthorizedly accessed in a ransomware attack, resulting in the unauthorized disclosure of the Personal Information of Plaintiff and the Class Members, including names, Social Security Numbers, and PII (the "Data Breach").[2]

3. As explained below, Plaintiff and Members of the Class have suffered significant injury and damages due to the Data Breach permitted to occur by Prospect, and the resulting misuse of their Personal Information and fraudulent activity, including monetary damages including out-of-pocket expenses, including those associated with the reasonable mitigation measures they were forced to employ, and other damages. Plaintiff and the Class also now forever face an amplified risk of *further* misuse, fraud, and identity theft due to their sensitive Personal Information falling into the hands of cybercriminals as a result of the tortious conduct of Defendant.

4. On behalf of herself and the Class preliminarily defined below, Plaintiff brings causes of action for negligence, negligence *per se*, breach of express and implied contractual duties, unjust enrichment, and invasion of privacy. Plaintiff seeks damages and injunctive and declaratory relief arising from Prospect's failure to adequately protect her highly sensitive Personal Information.

PARTIES

5. Plaintiff Roma is a natural person and citizen of the Commonwealth of Pennsylvania, residing in Springfield, Pennsylvania in the County of Delaware, where she intends to remain.

---

[2] *Id.*

6. Defendant, Prospect Medical Holdings, Inc. is a corporation with a principal place of business located at 3415 S. Sepulveda Boulevard, Los Angeles, California.

7. Prospect is a "fully integrated" healthcare corporation that provides healthcare to over 600,000 people.[3] Prospect "owns and operates 16 hospitals and more than 165 clinics and outpatient centers, with primary operations in California, Connecticut, Pennsylvania, Rhode Island and Texas."

8. Prospect owns and operates Crozer Health, a hospital system in Delaware County, Pennsylvania.[4]

9. Crozer Health provides inpatient and outpatient care "through its hospitals, ambulatory surgery centers, clinics, and doctors' offices across Delaware County."[5]

10. Plaintiff Roma is a former employee of Crozer Health, having been employed there from 2004 to 2015.

JURISDICTION AND VENUE

11. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because: (i) there are more than one hundred (100) Class Members; (ii) the aggregate amount in controversy exceeds five million dollars ($5,000,000.00), exclusive of interest and costs; and (iii) some Class Members are citizens of states different than Prospect.

12. This Court has personal jurisdiction over Prospect because it regularly and systematically transacts business in the Commonwealth of Pennsylvania, such that it can reasonably anticipate defending a lawsuit here. Moreover, this Court has jurisdiction over

---

[3] *Id.*

[4] https://www.crozerhealth.org/about/about-us/ (last accessed August 16, 2023).

[5] *Id.*

Defendant because its acts and omissions affected Plaintiff's property interests within Pennsylvania.

13. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to these claims occurred in this district, and/or or a substantial part of property that is the subject of this action is situated herein.

FACTUAL ALLEGATIONS

A. Plaintiff and the Class Members entrusted their Personal Information to Prospect

14. Plaintiff Roma and the Members of the proposed Class are present and former employees and prospective employees of Prospect.

15. From November 2004 to 2015, Roma was an employee at Crozer Health.

16. As a condition of employment, and/or of applying for employment with Crozer Health, Plaintiff and the Class Members were required by Crozer to confide and make available to it their sensitive and confidential Personal Information, including, but not limited to, their PII, names and Social Security Numbers, as well as financial information, bank routing number, and account number.

17. Prospect required that prospective employees provide their Personal Information when applying for employment.

18. Prospect acquired, collected, and stored a massive amount of said Personal Information of its employees, including Roma and the Members of the proposed Class, which it stored in its electronic systems.

19. By obtaining, collecting, using, and deriving a benefit from its employees' Personal Information, Prospect assumed legal and equitable duties to those individuals and knew or should have known that it was responsible for protecting their Personal Information from unauthorized

disclosure.

20. Plaintiff has taken reasonable steps to maintain the confidentiality of her Personal Information. Plaintiff, as a former employee, relied on Prospect to keep her Personal Information confidential and securely maintained, to use this information for authorized purposes and disclosures only.

21. Roma has never been the victim of another data breach.

22. Plaintiff and the proposed Class Members entrusted their Personal Information to Prospect solely for the purposes of applying for employment with Defendant and/or as a condition of employment, with the expectation and implied mutual understanding that Prospect would strictly maintain the confidentiality of the information and undertake adequate measures to safeguard it from theft or misuse.

23. Plaintiff and the proposed Class Members would not have entrusted Prospect with their highly sensitive Personal Information if they had known that Prospect would fail to take adequate measures to protect it from unauthorized use or disclosure.

B. Plaintiff's and the Class Members' Personal Information was Unauthorizedly Disclosed and Compromised in the Data Breach

24. As stated prior, Plaintiff Roma applied for employment with Prospect and was employed by Defendant for years from November 2004 to 2015.

25. As a prerequisite to employment, Plaintiff and the Class Members disclosed their non-public and sensitive Personal Information to Prospect, with the implicit understanding that their Personal Information would be kept confidential. This understanding was based on all the facts and circumstances attendant to their employment there, and the express, specific, written representations made by Prospect and its agents.

26. Plaintiff and the Class Members reasonably relied upon Prospect's representations

to her detriment and would not have provided their sensitive Personal Information to Prospect if not for Prospect's explicit and implicit promises to adequately safeguard that information.

27. On August 3, 2023, Prospect experienced a ransomware attack.[6] Crozer Health's computer systems were offline as a result of the attack.[7]

28. As of the date of this filing, according to the Crozer Health website, "Crozer Health, along with all Prospect Medical facilities, is [still] experiencing a systemwide outage."[8]

29. As of the date of this filing, Plaintiff Roma has not received formal notice of the Data Breach.

30. As a result of this Data Breach, the Personal Information of Plaintiff and the proposed Class Members, was unauthorizedly disclosed and compromised in the Data Breach.

31. As a result of the Data Breach, on August 9, 2023, Plaintiff received an alert from her Discover card services that her SSN was located on the Dark Web.

32. The Data Breach was preventable and a direct result of Prospect's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect employees' Personal Information.

33. In addition, as of the date of this filing, Plaintiff Roma has not received formal notice of the Data Breach, and upon information and belief, Prospect has not issued a formal written notice to anyone affected by the Data Breach.

C. The healthcare industry is a prime target for cybercriminals

---

[6] Ransomware hits Crozer Health and its owner Prospect Medical Holdings (inquirer.com). (last accessed August 16, 2023).

[7] *Id.*

[8] https://www.crozerhealth.org/ (last accessed August 21, 2023). See also, **Exhibit A**.

34. Over the past several years, data breaches have become alarmingly commonplace. In 2016, the number of data breaches in the U.S. exceeded 1,000, a 40% increase from 2015.[9] The next year, that number increased by nearly 50%.[10] The following year the healthcare sector was the second easiest "mark" among all major sectors and categorically had the most widespread exposure per data breach.[11]

35. The Personal Information stolen in the Data Breach is significantly more valuable than the loss of, say, credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Breach— most notably names and Social Security Numbers —is difficult, if not impossible, to change.

36. This kind of data, as one would expect, demands a much higher price on the dark web. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information… [is] worth more than 10x on the black market."[12]

37. PII data for sale is so valuable because PII is so broad, and it can therefore be used for a wide variety of criminal activity such as creating fake IDs, buying medical equipment and drugs that can be resold on the street, or combining PII with false provider numbers to file fake

---

[9] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, IDENTITY THEFT RESOURCE CENTER ("ITRC") (Jan. 19, 2017), https://www.idtheftcenter.org/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout/.

[10] *2017 Annual Data Breach Year-End Review*, ITRC, (Jan. 25, 2018), https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf.

[11] *2018 End-of-Year Data Breach Report*, ITRC, (Feb. 20, 2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

[12] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hackpersonal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

claims with insurers.

38. The value of Plaintiff's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

39. In fact, in June 2020, Crozer was the victim of a malware attack. "The organization said at the time that it had quickly isolated the problem, but trade publications that cover cybersecurity said some Crozer data was put up for auction after Crozer declined to pay ransom."[13]

40. Email phishing schemes "remain[] the primary attack vector for nine out of 10 cyberattacks."[14] Prospect did not elaborate on how the Data Breach happened, other than that three (3) employee email accounts were hacked.[15] Since "91% of ransomware attacks are the result of phishing exploits…" in the healthcare sector, it is more than plausible that the Data Breach was due to a phishing attack too.[16]

41. Companies can mount two primary defenses to phishing scams: employee education and technical security barriers.

42. Employee education is the process of adequately making employees aware of common phishing attacks and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known

---

[13] https://www.inquirer.com/health/crozer-health-computer-systems-down-20230803.html (last accessed August 21, 2023).

[14] Benishti, Eyal, *How to Safeguard Hospital Data from Email Spoofing Attacks*, INSIDE DIGITAL HEALTH, (Apr. 4, 2019), https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks.

[15] *See* n.32, *supra*.

[16] *Security Report Health Care – Hospitals, Providers and more*, CORVUS INSURANCE 2 (Mar. 3, 2020), https://info.corvusinsurance.com/hubfs/Security%20Report%202.2%20-%20Health%20Care%20.pdf.

recipients. Employee education and secure file-transfer protocols provide the easiest method to assist employees in properly identifying fraudulent e-mails and preventing unauthorized access to PII.

43. From a technical perspective, companies can also greatly reduce the flow of phishing e-mails by implementing certain security measures governing e-mail transmissions. Companies can use a simple email validation system that allows domain owners to publish a list of IP addresses that are authorized to send emails on their behalf to reduce the amount of spam and fraud by making it much harder for malicious senders to disguise their identities. Companies can also use email authentication that blocks email streams that have not been properly authenticated.

D. Prospect failed to sufficiently protect the Personal Information that Plaintiff and the Proposed Class Members Had Entrusted to It.

i. Prospect failed to adhere to FTC guidelines

44. According to the Federal Trade Commission("FTC"), the need for data security should be factored into all business decision-making.[17] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Prospect, should employ to protect against the unlawful exposure of Personal Information.

45. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[18] The guidelines explain that businesses should:

a. protect the personal information that they keep;

b. properly dispose of personal information that is no longer needed;

---

[17] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (Sep. 2, 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[18] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Sep. 28, 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

46. The FTC recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[19]

47. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

48. Prospect's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

ii. Prospect failed to adhere to industry standards

49. As stated above, the healthcare industry continues to be a high value target among cybercriminals. In 2017, the U.S. healthcare sector experienced over 330 data breaches, a number

[19] *See Start with Security*, *supra* n.40.

which continued to grow in 2018 (363 breaches).[20] The costs of healthcare data breaches are among the highest across all industries, topping $380 per stolen record in 2017 as compared to the global average of $141 per record.[21] As a result, both the government and private sector have developed industry best standards to address this growing problem.

50. The United States Department of Health and Human Services' Office for Civil Rights ("DHHS") notes that, "[w]hile all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations as they store large quantities of highly sensitive and valuable data."[22] DHHS highlights "several basic cybersecurity safeguards that can be implemented to improve cyber resilience which only require a relatively small financial investment, yet they can have a major impact on an organization's cybersecurity posture."[23] Most notably, organizations must properly encrypt PII in order to mitigate against misuse.

51. The private sector has similarly identified the healthcare sector as particularly vulnerable to cyber-attacks both because of the of value of the PII that it maintains and because, as an industry, it has been slow to adapt and respond to cybersecurity threats.[24]

52. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, Prospect failed to adopt sufficient data security processes.

53. Prospect failed to adequately train its employees on even the most basic of

---

[20] 2018 End of Year Data Brach Report, ITRC, (Feb. 20, 2019), https://www.idtheftcenter.org/ wp-content/uploads/2019/02/ITRC_2018-End-of-Year Aftermath_FINAL_V2_ combinedWEB.pdf.
[21] *Ibid.*
[22] *Cybersecurity Best Practices for Healthcare Organizations*, HIPAA JOURNAL (Nov. 1, 2018), https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/.
[23] *Id.*
[24] *10 Cyber Security Best Practices For the Healthcare Industry*, NTIVA (Jun. 19, 2018), https://www.ntiva.com/blog/10-cybersecurity-best-practices-for-the-healthcare-industry.

cybersecurity protocols, including:

a. How to detect phishing emails and other scams including providing employees examples of these scams and guidance on how to verify if emails are legitimate;

b. Effective password management and encryption protocols for internal and external emails;

c. Avoidance of responding to emails that are suspicious or from unknown sources;

d. Locking, encrypting and limiting access to computers and files containing sensitive information; and

e. Implementing guidelines for maintaining and communicating sensitive data.

54. Prospect's failure to implement these rudimentary measures made it an easy target for the Data Breach that came to pass.

E. Plaintiff and the Class Members were significantly injured by the Data Breach

55. As a result of Prospect's failure to prevent the Data Breach, Plaintiff Roma and the Class Members have suffered and will continue to suffer significant injury and damages. They have suffered or are at increased risk of suffering:

a. Misuse of Personal Information, including Ms. Roma's SSN being located on the Dark Web by Discover;

b. An increased number of spam texts and phone calls;

c. Decrease in credit scores;

d. The loss of the opportunity to control how Plaintiff's and the Class

Members' Personal Information is used;

e. The diminution in value of their Personal Information;

f. The compromise, publication and/or theft of their Personal Information;

g. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud, including the purchase of identity theft protection insurance and detection services;

h. Lost opportunity costs and lost wages associated with the time and effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

i. Delay in receipt of tax refund monies;

j. Unauthorized use of stolen Personal Information;

k. The continued risk to their Personal Information, which remains in the possession of Prospect and is subject to further breaches so long as it fails to undertake appropriate measures to protect the Personal Information in their possession; and

l. Current and future costs related to the time, effort, and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

56. As a result of the Data Breach, Plaintiff and the Class Members now face, and will continue to face, a heightened risk of identity theft and fraud for the rest of their lives.

57. As a long-standing member of the healthcare community, Prospect knew or should

have known the importance of safeguarding patient Personal Information entrusted to it and of the foreseeable consequences of a breach. Despite this knowledge, however, Prospect failed to undertake adequate cyber-security measures to prevent the Data Breach email attack from happening.

58. On the contrary, after conducting a study, the U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[25]

CLASS ACTION ALLEGATIONS

59. Plaintiff brings this action on behalf of herself and all others similarly situated pursuant to Fed. R. Civ. Proc. 23. The Class is preliminarily defined as:

> All individuals whose Personal Information was compromised as a result of the Data Breach with Prospect which was announced on or about August 3, 2023.

60. Excluded from the Class are Prospect and its subsidiaries and affiliates, officers, directors, and members of their immediate families, and any entity in which it has a controlling interest, the legal representatives, heirs, successors or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

61. Plaintiff reserves the right to modify or amend the definition of the proposed Class and/or to add a subclass(es) if necessary, before this Court determines whether certification is appropriate.

62. *Fed. R. Civ. Proc. 23(a)(1) Numerosity:* The Class is so numerous such that joinder

---

[25] *Victims of Identity Theft, 2012*, U.S. DEP'T OF JUSTICE 10, 11 (Jan. 27, 2014), https://www.bjs.gov/content/pub/pdf/vit12.pdf.

of all Members is impracticable. Upon information and belief, and subject to class discovery, the Class consists of 13,770 current and former employees of Prospect, the identity of whom are within the exclusive knowledge of and can be ascertained only by resort to Prospect's records. Prospect has the administrative capability through its computer systems and other records to identify all Members of the Class, and such specific information is not otherwise available to Plaintiff.

63. *Fed. R. Civ. Proc. 23(a)(2) Commonality and Fed. R. Civ. Proc. 23(b)(3) Predominance:* There are numerous questions of law and fact common to the Class. As such, there is a well-defined community of interest among the Members of the Class. These questions predominate over questions that may affect only individual Members of the Class because Prospect has acted on grounds generally applicable to the Class. Such common legal or factual questions include, but are not limited to:

a. Whether Prospect had a duty to protect employee Personal Information;

b. Whether Prospect knew or should have known of the susceptibility of its systems to a data breach;

c. Whether Prospect's security measures to protect its systems were reasonable considering best practices recommended by data security experts;

d. Whether Prospect was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Prospect's failure to implement adequate data security measures allowed the Data Breach to occur;

f. Whether Prospect's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach, resulting in the unlawful exposure

of the Plaintiff's and Class Members' Personal Information;

g. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of Prospect's failure to reasonably protect its systems and data network;

h. Whether Plaintiff and Class Members are entitled to relief;

i. Whether Prospect failed to adequately notify Class Members of the compromise of their Personal Information;

j. Whether Prospect assumed a fiduciary duty and/or confidential relationship to Class Members when they entrusted it with their Personal Information;

k. Whether Prospect breached its contracts with Class Members by failing to properly safeguard their Personal Information and by failing to notify them of the Data Breach;

l. Whether Prospect's violation of FTC regulations constitutes evidence of negligence or negligence *per se*;

m. Whether Prospect impliedly warranted to Class Members that the information technology systems were fit for the purpose intended, namely the safe and secure processing of Personal Information, and whether such warranty was breached.

64. *Fed. R. Civ. Proc. 23(a)(3) Typicality:* Plaintiff's claims are typical of the claims of all Class Members, because all such claims arise from the same set of facts regarding Prospect's failures:

a. to protect Plaintiff's and Class Members' Personal Information;

b. to discover and remediate the security breach of its computer systems more

quickly; and

c. to disclose to Plaintiff and Class Members in a complete and timely manner information concerning the security breach and the theft of their Personal Information.

65. *Fed. R. Civ. Proc. 23(a)(4) Adequacy:* Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff is a more than adequate representative of the Class in that Plaintiff is a victim of the Data Breach, has suffered injury and damages such as misuse and fraudulent activity as a result of the Data Breach, and brings the same claims on behalf of herself and the putative Class. Plaintiff has no interests antagonistic to that of the Class Members. Plaintiff has retained counsel who are competent and experienced in litigating class actions, including class actions following data breaches and unauthorized data disclosures. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

66. *Fed. R. Civ. Proc. 23(b)(2) Injunctive and Declaratory Relief:* Prospect has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

67. *Fed. R. Civ. Proc. 23(b)(3) Superiority:* It is impracticable to bring Class Members' individual claims before the Court. Class treatment permits many similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort, expense, or the possibility of inconsistent or contradictory judgments that numerous individual actions would engender. The benefits of the class mechanism, including providing injured persons or entities with a method for obtaining redress on claims that might not be practicable to pursue individually, substantially outweigh any difficulties that may arise in the management of this class action.

68. A class action is superior to the other available methods for the fair and efficient adjudication of this controversy because:

a. The unnamed Members of the Class are unlikely to have an interest in individually controlling the prosecution of separate actions;

b. Concentrating the litigation of the claims in one forum is desirable;

c. Plaintiff anticipates no difficulty in the management of this litigation as a class action; and

d. Plaintiff's legal counsel has the financial and legal resources to meet the substantial costs and legal issues associated with this type of litigation.

69. Plaintiff knows of no unique difficulty to be encountered in the prosecution of this action that would preclude its maintenance as a class action.

70. *Fed. R. Civ. Proc. 23(c)(4) Issue Certification:* Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether Prospect owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing and safeguarding their Personal Information;

b. Whether Prospect's security measures to protect its data systems were reasonable considering best practices recommended by data security experts;

c. Whether Prospect's failure to institute adequate protective security measures amounted to negligence;

d. Whether Prospect failed to take commercially reasonable steps to safeguard

prospective employee and employee Personal Information; and

e. Whether adherence to FTC data security recommendations, and industry standards on data security would have reasonably prevented the Data Breach.

71. Finally, all Members of the proposed Class are readily ascertainable. Prospect has access to employee and applicant names and addresses affected by the Data Breach. Using this information, Class Members can be identified and ascertained for the purpose of providing constitutionally sufficient notice.

COUNT I
NEGLIGENCE

72. Plaintiff Roma and the Members of the Class incorporate the above allegations as if fully set forth herein.

73. Defendant Prospect owed a duty to Plaintiff and the Members of the Class to exercise reasonable care to safeguard their Personal Information in its possession, based on the foreseeable risk of a data breach and the resulting exposure of their information, as well as on account of the special relationship between Defendant and its employees, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

74. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Members of the Class's Personal Information by disclosing and providing access to this information to third parties and by failing to properly supervise both the manner in which the information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

75. Further, Defendant owed to Plaintiff and Members of the Class a duty to notify them within a reasonable time frame of any breach to the security of their Personal Information. Defendant also owed a duty to timely and accurately disclose to Plaintiff and Members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and Members of the Class to take appropriate measures to protect their Personal Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the harm caused by the Data Breach.

76. Prospect owed these duties to Plaintiff and Members of the Class because they are Members of a well-defined, foreseeable, and probable class of individuals who Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and Members of the Class's personal information and PII for employment purposes.

77. Plaintiff and Members of the Class were required to provide their Personal Information to Defendant as a condition of applying for employment and/or as a condition of employment, and Defendant retained that information.

78. The risk that unauthorized persons would attempt to gain access to the Personal Information and misuse it was foreseeable. Given that Defendant holds vast amounts of this information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Personal Information, whether by email hacking attack, or otherwise.

79. Personal Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Personal Information of Plaintiff and Members of the Class, and the importance of exercising reasonable care in handling it.

80. Defendant Prospect breached its duties by failing to exercise reasonable care in supervising its employees and agents, and in handling and securing the Personal Information and PII of Plaintiff and Members of the Class which actually and proximately caused the Data Breach and Plaintiff's and Members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and Members of the Class's injuries-in-fact.

81. As a direct, proximate, and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Members of the Class have suffered or will suffer injury and damages, including misuse and fraudulent activity, monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

82. Defendant's breach of its common law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff's and Members of the Class's actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
NEGLIGENCE *PER SE*

83. Plaintiff and the Class Members incorporate the above allegations as if fully set forth herein.

84. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class

Members' Personal Information, PII.

85. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, employees' and prospective employees' PII.

86. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Class Members' sensitive PII.

87. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect its employees' and prospective employees' PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had required and solicited, collected, and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to employees in the event of a breach, which ultimately came to pass.

88. The harm that has occurred in the Data Breach is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class Members.

89. Defendant had a duty to Plaintiff and the Class Members to implement and maintain reasonable security procedures and practices to safeguard their PII.

90. Defendant breached its respective duties to Plaintiff and Members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class Members' PII.

91. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

92. But-for Prospect's wrongful and negligent breach of its duties owed to Plaintiff and the Class, Plaintiff and the Members of the Class would not have been injured.

93. The injury and harm suffered by Plaintiff and the Class Members were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and Members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

94. Had Plaintiff and Members of the Class known that Defendant did not adequately protect employees' and prospective employees' PII, Plaintiff and Members of the Class would not have entrusted Defendant with their PII.

95. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class Members have suffered harm, injury, and damages as set forth in the preceding paragraphs.

COUNT III
BREACH OF EXPRESS/IMPLIED CONTRACTUAL DUTY

96. Plaintiff and Members of the Class incorporate the above allegations as if fully set forth herein.

97. Defendant offered to provide employment to Plaintiff and Members of the Class in exchange for payment.

98. Prospect also required Plaintiff and the Members of the Class to provide Defendant with their Personal Information as a condition of applying for employment, and for employees as a condition of receiving renumeration for labor rendered.

99. In turn, Defendant agreed it would not disclose Personal Information it collects to unauthorized persons. Defendant also promised to maintain safeguards to protect their Personal

Information.

100. Plaintiff and the Members of the Class accepted Defendant's offer by providing Personal Information to Prospect, in applying for employment, and providing labor to Defendant and receiving renumeration.

101. The agreement was supported by adequate consideration, as it was an exchange of labor for money.

102. Implicit in the Parties' agreement was that Defendant would provide Plaintiff and Members of the Class with prompt and adequate notice of any and all unauthorized access and/or theft of their Personal Information.

103. Plaintiff and the Members of the Class would not have entrusted their Personal Information to Defendant in the absence of such agreement with Defendant.

104. Prospect materially breached the contract(s) it had entered with Plaintiff and Members of the Class by failing to safeguard such Personal Information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant further breached the implied contracts with Plaintiff and Members of the Class by:

a. Failing to properly safeguard and protect Plaintiff' and Members of the Class's Personal Information;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement;

c. Failing to ensure the confidentiality and integrity of electronic Personal Information that Defendant received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1).

105. The damages sustained by Plaintiff and Members of the Class as set forth in the

preceding paragraphs were the direct and proximate result of Defendant's material breaches of its agreement(s).

106. Plaintiff and Members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

107. The covenant of good faith and fair dealing is implied into every contract. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

108. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

109. Defendant failed to advise Plaintiff and Members of the Class of the Data Breach promptly and sufficiently.

110. In these and other ways, Defendant violated its duty of good faith and fair dealing.

111. Plaintiff and Members of the Class have sustained damages as a result of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

COUNT IV
UNJUST ENRICHMENT

112. Plaintiff and Members of the Classes incorporate the above allegations as if fully set forth herein.

113. This claim is pleaded in the alternative to the breach of express/implied contractual

duty claim.

114. Plaintiff and Members of the Classes conferred a benefit upon Defendant in the form of labor rendered in exchange for renumeration.

115. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and Members of the Class. Defendant also benefited from the receipt of Plaintiff's and Members of the Class's Personal Information, as this was required to facilitate the employment relationship and renumeration, as well as for the purpose of applying for employment.

116. As a result of Defendant's conduct, Plaintiff and Members of the Class suffered actual damages in an amount equal to the difference in value between the value of their labor with reasonable data privacy and security practices and procedures that Plaintiff and Members of the Classes were entitled to, and that labor without unreasonable data privacy and security practices and procedures that they received.

117. Under principals of equity and good conscience, Defendant should not be permitted to retain the monetary value of the labor belonging to Plaintiff and Members of the Classes because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures for itself for which Plaintiff and Members of the Classes expended labor and that were otherwise mandated by federal, state, and local laws and industry standards.

118. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V
INVASION OF PRIVACY

119. Plaintiff and Members of the Class incorporate the above allegations as if fully set forth herein.

120. Defendant publicized private details and facts not generally known to the public, not publicly available, and not of legitimate public concern about Plaintiff and the Class Members by disclosing and exposing Plaintiff's and the Class Members' Personal Information to enough people that it is reasonably likely those facts have and/or will become known to the public at large, including, without limitation, on the dark web and elsewhere.

121. The disclosure of employees' and prospective employees' full names, Social Security numbers, and financial information, is particularly harmful and would be offensive to a reasonable person of ordinary sensibilities.

122. Defendant has a special relationship with Plaintiff and the Class Members and Defendant's disclosure of Personal Information is certain to embarrass them and offend their dignity. Defendant should appreciate that the cyber-criminals who stole the Personal Information would fraudulently misuse that Personal Information, and further sell and disclose the data, just as they are doing. That the original disclosure is devastating to the Plaintiff and the Class Members, even though it originally may have only been disclosed to one person or a limited number of cyber-criminals, does not render it any less a disclosure to the public-at-large considering that said non-public information is now made public, and cannot be secured again.

123. Plaintiff's and the Class Members' Personal Information was publicly disclosed by Defendant in the Data Breach with reckless disregard for the reasonable offensiveness of the disclosure. Such disclosure is highly offensive and would be to any person of ordinary sensibilities. Defendant knew or should have known that Plaintiff's and the Class Members' PII is not a matter of legitimate public concern.

124. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been injured and are entitled to damages, as set forth herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, JOANNE ROMA, individually and on behalf of all others similarly situated, the Class as heretofore identified, respectfully prays this Honorable Court for judgment as follows:

A. Certification for this matter to proceed as a class action on behalf of the proposed Class under Fed. R. Civ. Proc. 23;

B. Designation of Plaintiff as Class Representatives and designation of the undersigned as Class Counsel;

C. Actual damages in an amount according to proof;

D. Injunctive or declaratory relief;

E. Pre- and post-judgment interest at the maximum rate permitted by applicable law;

F. Costs and disbursements assessed by Plaintiff in connection with this action, including reasonable attorneys' fees pursuant to applicable law;

G. For attorneys' fees under the common fund doctrine and all other applicable law; and

H. Such other relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the Class, hereby demand a trial by jury pursuant to Fed. R. Civ. Proc. 38(b) on all claims so triable.

Dated: August 21, 2023

Respectfully submitted,

BY: */S/ Patrick Howard*

Patrick Howard (PA ID #88572)
SALTZ, MONGELUZZI, & BENDESKY, P.C.
1650 Market Street, 52nd Floor
Philadelphia, PA 19103
Tel: (215) 496-8282

Fax: (215) 496-0999
phoward@smbb.com

J. Gerard Stranch, IV*
Andrew Mize*
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com

Counsel for Plaintiff and the Proposed Class

**Pro Hac Vice forthcoming*